Summary

[059] A computer network is made more secure from attack attacks by partitioning the network into sub-networks and placing firedoors in association with the links that connect each sub-network to areas outside the sub-network. The firedoors scan traffic that flows through these links to identify – based on pre-stored pattern information – whether the traffic contains a virus, or some other attack, and blocks it from leaving the sub-network. The firedoors are coupled to a firedoor keeper, through which a firedoor informs the firedoor keeper whenever it detects unusual activity that suggests a successful virus breach of the protection intended for the gateway's network and, conversely, the firedoor keeper updates a pre-stored patterns file in all of the firedoors, or directs the firedoors to take specific action, e.g., blocking all traffic, whenever the firedoor keeper deemed it necessary.